

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hirofumi MURATANI, et al.

SERIAL NO: NEW APPLICATION

GAU:

FILED: HEREWITH

EXAMINER:

FOR: ENCRYPTION APPARATUS, DECRYPTION APPARATUS, EXPANDED KEY GENERATING APPARATUS AND METHOD THEREFOR, AND RECORDING MEDIUM



**INFORMATION DISCLOSURE/RELATED CASE STATEMENT UNDER 37 CFR 1.97**

ASSISTANT COMMISSIONER FOR PATENTS  
WASHINGTON, D.C. 20231

SIR:

Applicant(s) wish to disclose the following information.

**REFERENCES**

- ☒ The applicant(s) wish to make of record the references listed on the attached form PTO-1449. Copies of the listed references are attached, where required, as are either statements of relevancy or any readily available English translations of pertinent portions of any non-English language references.
- ☐ A check is attached in the amount required under 37 CFR §1.17(p).

**RELATED CASES**

- ☐ Attached is a list of applicant's pending application(s) or issued patent(s) which may be related to the present application. A copy of the patent(s), together with a copy of the claims and drawings of the pending application(s) is attached along with PTO 1449.
- ☐ A check is attached in the amount required under 37 CFR §1.17(p).

**CERTIFICATION**

- ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement.
- ☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application or, to the knowledge of the undersigned, having made reasonable inquiry, was known to any individual designated in 37 CFR §1.56(c) more than three months prior to the filing of this statement.

**DEPOSIT ACCOUNT**

- ☒ Please charge any additional fees for the papers being filed herewith and for which no check is enclosed herewith, or credit any overpayment to deposit account number 15-0030. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

Marvin J. Spivak  
Registration No. 24,913



**22850**

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 10/98)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Hirofumi MURATANI, et al.

SERIAL NO.: NEW APPLICATION

FILED: HERewith

FOR: ENCRYPTION APPARATUS, DECRYPTION APPARATUS,  
EXPANDED KEY GENERATING APPARATUS AND  
METHOD THEREFOR, AND RECORDING MEDIUM

**STATEMENT OF RELEVANCY**

**Reference AW(Alfred J. MENEZES, et al.) on form PTO-1449:**

This textbook describes the key schedule of DES. This key schedule is basically realized by bit rotation. After 16 rounds, the state of the key schedule go back to the initial state. Because of this circularity, the key schedule of decryption is realized by the reverse bit rotation.

Form PTO 1449 (Modified)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTY DOCKET NO. 211428US2SRD		SERIAL NO. NEW APPLICATION	
LIST OF REFERENCES CITED BY APPLICANT				APPLICANT Hirofumi MURATANI, et al.			
				FILING DATE HEREWITH		GROUP	
<b>U.S. PATENT DOCUMENTS</b>							
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
	AL						
	AM						
	AN						
<b>FOREIGN PATENT DOCUMENTS</b>							
		DOCUMENT NUMBER	DATE	COUNTRY	TRANSLATION YES NO		
	AO						
	AP						
	AQ						
	AR						
	AS						
	AT						
	AU						
	AV						
<b>OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, etc.)</b>							
	AW	Alfred J. MENEZES, et al., HANDBOOK OF APPLIED CRYPTOGRAPHY, Chapter 7 Block Ciphers, pgs. 250-259					
	AX						
	AY						
	AZ						
Examiner					Date Considered		
<small>*Examiner: Initial if reference is considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.</small>							

09/902596  
 07/12/01